EXHIBIT 1

About InfoWorld : Advertise : Subscribe : Contact Us : Awar

II

InfoWorld

HOME NEWS TEST CENTER OPINIONS PRODUCT GUIDE TECHINDEX

PRODUCT REVIEWS GUIDE | REVIEWS | ANALYSES | SPECIAL REPORTS

● Site ○ IT Product Guide

□ Technology & Business I

□ SOA Report

Enter Email Address

EnCase keeps tabs on compliance complexity

Flexible forensics tools closely tracks and records incidents

By Oliver Rist , Brian Chee
October 08, 2004

It's a sad fact that many a network manager will skip this review. This in spite of Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley. This in spite of identity theft, corporate espionage, and a bucket full of other white-collar crimes. Network managers will avoid this review because these are worst-case scenarios, and it's easier not to think about them than it is to rationally consider their potential costs. Mitigating these costs, both soft and hard dollar, is precisely what **Guidance Software's** (Profile, Products, Articles) EnCase Enterprise Edition is designed to handle.

Guidance Software EnCase Enterprise Edition

Guidance Software describes EnCase as a "network-enabled forensics, incident response, and security analysis tool." Not only capable of ensuring your systems are properly patched, EnCase is fed by your intrusion detection system to closely track attacks and record them with snapshots for later review. Further, EnCase is an excellent tool for automating compliance testing for stringent regulations such as HIPAA. Companies can quickly search through servers and workstations from a single console for sensitive documents and images, then determine how files have been distributed through the enterprise and by whom.

SEE ALSO

- **Government publishes HI standards**
- **Cutting the Sarbanes-Oxl**

» COMPLETE LIST OF TAGS

FIND PRODUCTS AND COM

» COMPLETE PRODUCT GUIDE

TECHNOLOGY INDEX

- Applications
- Application Development
- Security
- Networking
- Wireless
- Platforms
- Hardware
- Data Management
- Storage
- Web Services
- Business
- Telecom
- Professional Services
- Standards

TECH WATCH RSS

Guidance Software,
http://guidancesoftware.com/

Very Good 7.7

criteria	score	weight
Features	9	25%
Manageability	7	20%
Performance	8	20%
Integration	7	15%
Documentation	7	10%
Value	7	10%

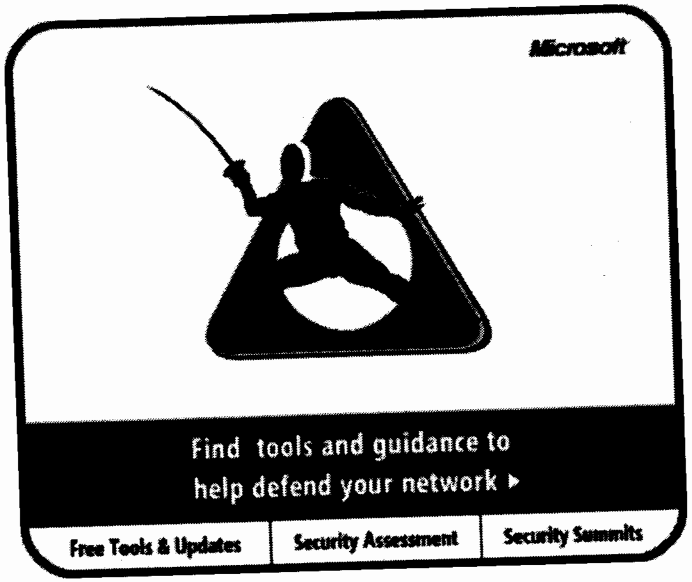
Cost:
$1,600 per seat, as tested

Platforms:
Linux (kernel 2.4), Solaris v8 and v9 (32-bit and 64-bit), Windows NT/2000/XP/2003

Bottom Line:
EnCase's roots in law enforcement combined with its capability of integrating with enterprise intrusion detection systems makes this one of the more flexible and easily integrated forensic solutions for the enterprise. Although it's very complex, this type of software is a must-have for companies faced with compliance issues.

About our Reviews and Scoring Methodology

EnCase consists of three components: the SAFE (Secure Authentication For EnCase) Server, the Examiners, and the Servlets. Using a police metaphor, the SAFE Server can be viewed as headquarters. This server manages authentication and secure communication among all other system components and stores EnCase log files for future analysis. The Examiners can be looked at as precinct houses. They're in charge of specific network segments or resources, depending on how you've architected your EnCase deployment. They also act as command consoles for analysis and incident response. The Servlets are the field detectives. They're installed on all EnCase-protected servers and workstations running OSes including Linux, Solaris, and Windows. Servlets watch out for trouble, gather information, and send out alerts.



Each component communicates using TCP/IP port 4445 with asymmetrical encryption (certificates) and USB license dongles at the Examiner and SAFE Server stations. Licensing depends upon how many simultaneous examiners and SAFE Servers you want for your enterprise. With a single license, only one person at a time may examine data. This is certainly a flexible design, but it means that there's no such thing as a typical EnCase installation; pricing can vary widely from organization to organization.

Casing the Joint

We tested EnCase in the wild, opening it up to four different class C subnets across the University of Hawaii's production network. Once installed, we used EnCase to run vulnerability and patch compliance tests against our Linux and Windows test machines.

The Examiner station also allowed us to browse files on each machine. This feature includes the capability of displaying thumbnails of any images stored on the machine, whether current or recently deleted. We also compared the hash values from EnCase's library to determine whether any sensitive files, such as the Windows directory or the virus scanner, had been modified. This often occurs in Trojan horse attacks, in which malware substitutes critical files with corrupted ones.

EnCase also allowed us to search for known corrupted or attack-based files on our machines using keywords, hash values, hex strings from headers and partial headers; we also could search with manual browsing.

Searching for specific documents requires subject-matter expertise on the part of the user in order to formulate the properly phrased search questions; the well-designed GUI makes this easier. Adminis can delegate search authority to different people within the organization; the HR administrator, for instance, might appropriately be given rights to search through all HR documents.

Telecommuters are less sec
People who work remotely are productive, they are more likel Don't take my word for it - tha survey by Insight Express and reported in EE Times. While 76 employees surveyed ...

Compuware plans EclipseC
The EclipseCon 2006 conferen the week of March 20 in Santa and it looks like Compuware h this event. Compuware and Ec representatives are being mos about Compuware's plans. But

JON UDELL'S CORNER

Sidestepping th
(InfoWorld) - On a "The West Wing," security adviser K McCormack) repri

Jon's Blog | Jon's Column

COLUMNISTS

Dell gets petitioned, HP's p

(InfoWorld) - Gre Microsoft is rolling of vista when it a millennium....

» MORE COLUMNISTS

MORE INFOWORLD BLOGS

Open Sources
Is selling your open source ticket to freedom?
Sarah Lacy's Open Season On talks about some of the recent acquisitions and the impact th

The Deep End
DNSBL Stats
For an upcoming article, I four to gather some statistics on DI spamhaus.org, sorbs.net, and

EnCase also features EnScript, a Perl/Java-like scripting language. Using EnScript, admins can customize searches of any combination of single or multiple machines for all documents meeting specific criteria, including size, keywords, extension type, and even the destination of the data. Thus an admin could craft a script that tracks documents containing the keywords "social security number" and whether an employee attempts to distribute them to improper departments or outside the organization.

Administrators can set up EnCase to automatically monitor specific machines or groups for certain conditions, such as file alterations, rapid port probes, and more. If EnCase detects these activities, it can grab snapshots of the machine while the attack is in progress. By simply looking at a case file, admins can clearly view at a later time the attack's entire progression. EnCase can be integrated with **Internet Security Systems'** (Profile, Products, Articles) intrusion detection product or Snort for managing attack thresholds, making the feature all the more useful.

Case evidence and disk snapshots can be stored on just about any file system you wish. Snapshot information can also be mounted as a read-only volume, designed as a way to gather immediate evidence for later analysis.

Using the stand-alone EnCase Professional Edition, you can produce a case file to submit to a local law enforcement agency. Case files can pertain to any number of incidents, such as a worm break or a case of an employee sending sensitive documents to an inappropriate recipient. Case files can contain various types of data, and they're locked up and protected from unauthorized access. In a nice touch, these case files are open enough to accept additional data from other EnCase instances.

Additionally, each Examiner account can be given varying levels of access to examination functions. So a junior engineer might only able to take and store system snapshots, whereas a user with higher access privileges can later peel apart the images to create the case evidence.

Although the field of corporate computer-forensic products is rather new, the EnCase software is surprisingly mature. Installation completed without incident, and even during operation we encountered only minor hiccups. For instance, it didn't correctly identify our Linux test machine as running Slackware, but it did correctly identify the Linux kernel version.

Also, EnCase didn't directly support FreeBSD, one of the other platforms on which we tested. However, we were able to work around that, because EnCase allows admins to perform a manual forensic copy, which is essentially taking a snapshot of the entire disk image (regardless of OS) using a directly attached slave drive, or a USB or network connection.

Finally, EnCase is remarkably complex. The company might seriously consider producing some tutorials on CD or some documentation featuring example data.

Forensic software such as EnCase began in the law enforcement field. But with the grave increase in computer crime -- especially from inside the firewall -- such systems are often necessary for effective security. Further, EnCase provides an easy and centrally managed method for compliance testing with an automatic results store throw in. For many enterprises, solutions such as EnCase might be considered a security luxury; but for trading companies, banks, and even companies that merely keep a large amount of customer financial data, EnCase is a must.

Oliver Rist is a senior contributing editor at *InfoWorld*.

- **Advice Line**
- **Database Underground**
- **The Deep End**
- **Enterprise Mac**
- **Grid Meter**
- **The Gripe Line**
- **InfoWorld Daily**
- **Inside IT**
- **IT Troubleshooter**
- **Jon's Radio**
- **Open Sources**
- **Real World SOA**
- **Security Adviser**
- **SMB IT**
- **The Storage Network**
- **Tech Watch**
- **Zero Day**

IDG ENTERPRISE NETWORK

- Riding The California Priva

TOP NEWS:

» **Cell phone ticketing coming to Germany**
The airline DBA's passengers will be able to check in and board flights on the Munich-Hanover route with mobile phones capable of receiving MMS

» **Borland: Interest, but no buyer yet, for tools line**
Executive details intentions, provides progress report on sale of developer tools

» **Intel gives earnings warning**
Intel faces increasing competition from AMD

» **Update: Google shrinks further the Mini search device**
Google introduces its lowest-priced search device to date

» **HP Labs India working to bridge TV and Internet**
Also in Brief: OSS/J names Vodafone D2 exec as new chair; IBM readies SOA packages; Intel to invest $300M in Vietnam chip plant; SOA, Forum integrate products; Ericsson sues Samsung in patent dispute; Sony, NEC to establish optical disc joint venture; Orange offers wireline service

» **Vendors form new OpenDocument alliance**
ODF could have provided support to embattled CIO who planned Massachusetts' migration to OpenDocument

FREE SUBSCRIPTION

Order today to get your **FREE subscription** (a $195 value!) to InfoWorld magazine, the weekly publication that provides indispensable product information to IT professionals.

NOTE: Complimentary subscriptions sent only to those applicants who qualify.

First Name:

Last Name:

Company Name:

Title:

Mailing Address:

City:

State/Province:

Select One

Zip/Postal Code:

Email Address:

NOTE: Offer valid in U.S. and Canada only
Non-U.S. click here

HOME | NEWS | TEST CENTER | OPINIONS | PRODUCT GUIDE | TECHINDEX

About :: Advertise :: Subscribe :: Contact Us :: Awards :: Events

Computerworld :: Network World :: CIO :: PC World :: Darwin :: CMO :: CSO :: Bio-IT World
IT Careers :: JavaWorld :: Macworld :: Mac Central :: Playlist :: GamePro :: GameStar :: Gamerhelp
ITWorld Canada :: Computerwoche :: Techworld UK :: tecChannel :: IDG.se :: IDG.no

site: testcenter zone: feature pkeys: pkey=security; skeys: skey=computer_forensics;skey=patch_management; tdata: kw=; tid: